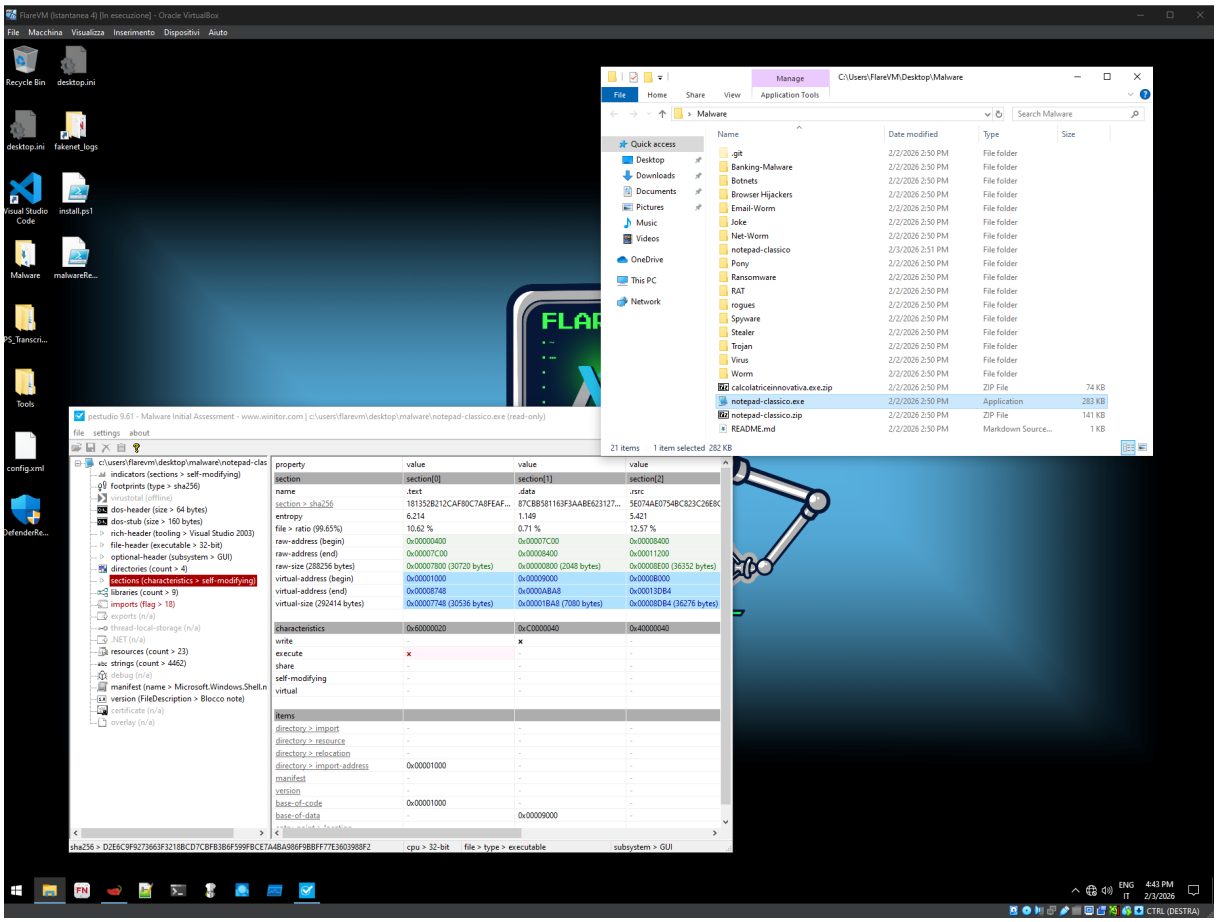
Report Tecnico:
Malware Analysis Statica

Target: File Eseguibile "notepad-classico.exe"

Autore: Josh Van Edward D Abanico
Data: 3 febbraio 2026



Obiettivo: Analisi delle Librerie (Imports) e delle Sezioni (PE Headers)
Strumenti Utilizzati: FlareVM, PEStudio

Indice

1 Introduzione e Obiettivi **2**
1.1 Scenario 2
1.2 Hash del File 2

2 Fase 1: Analisi delle Librerie (Imports) **2**
2.1 Librerie Standard 2
2.2 Funzioni Sospette e Flag Critici 3

3 Fase 2: Analisi delle Sezioni (PE Headers) **3**
3.1 Anomalie Rilevate 3

4 Conclusioni **4**

1 Introduzione e Obiettivi

1.1 Scenario

L'obiettivo di questa attività è analizzare un file sospetto denominato `notepad-classico.exe`. Il file si presenta come un comune editor di testo, ma è sospettato di contenere funzionalità malevole nascoste. L'analisi è stata condotta in un ambiente isolato (FlareVM) utilizzando tecniche di analisi statica.

1.2 Hash del File

- **Nome File:** notepad-classico.exe
- **Contesto:** Esercitazione Malware Analysis

2 Fase 1: Analisi delle Librerie (Imports)

2.1 Librerie Standard

L'analisi preliminare tramite **PEStudio** mostra che il malware importa diverse librerie standard di Windows per simulare un comportamento legittimo. Sono presenti `comdlg32.dll` e `SHELL32.dll`, che forniscono le finestre di dialogo "Apri/Salva" e funzionalità di Drag & Drop, tipiche di un Notepad reale.

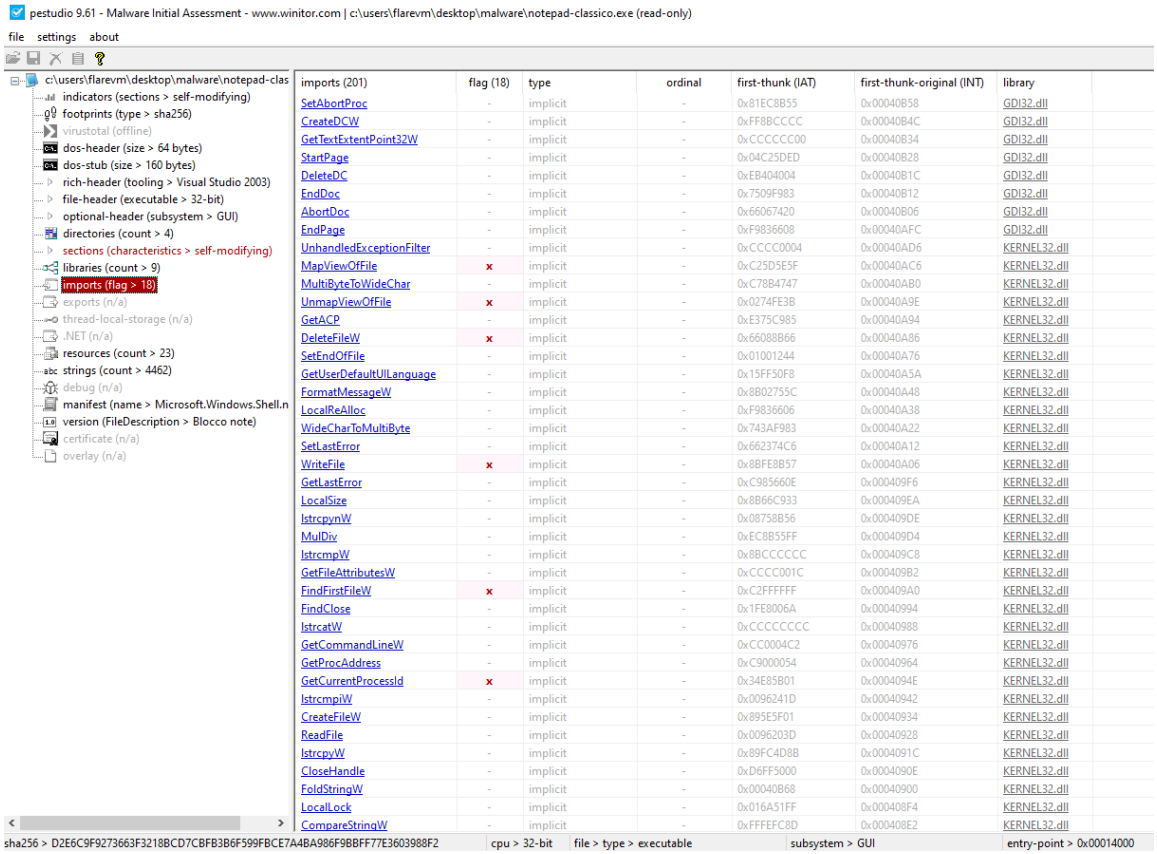


Figura 1: Librerie grafiche e di interfaccia utente.

2.2 Funzioni Sospette e Flag Critici

Approfondendo l'analisi della Import Address Table (IAT), PEStudio segnala numerosi **Red Flag** su funzioni critiche, in particolare nelle librerie `KERNEL32.dll` e `ADVAPI32.dll`.

Le funzioni più rilevanti identificate sono:

- **Gestione File e Memoria (KERNEL32.dll):**
  - `DeleteFileW`: Permette al programma di eliminare file dal disco. Comportamento anomalo per un editor di testo, spesso usato dai malware per cancellare le proprie tracce (self-deletion).
  - `MapViewOfFile` / `UnmapViewOfFile`: Utilizzate per mappare file in memoria. Queste API sono spesso sfruttate per tecniche di *Process Injection* (es. Process Hollowing).
- **Persistenza (ADVAPI32.dll):**
  - `RegCreateKeyW` / `RegSetValueExW`: Funzioni che permettono di scrivere nel Registro di Sistema. I malware le utilizzano per garantirsi la **persistenza**, aggiungendosi alle chiavi di avvio automatico (es. *Run keys*).
- **Monitoraggio (USER32.dll):**
  - `SetWinEventHook`: Può essere usata per intercettare input dell'utente (comportamento simil-keylogger).
  - `GetForegroundWindow`: Permette di sapere quale finestra l'utente sta utilizzando, tecnica usata dai banking trojan.

3 Fase 2: Analisi delle Sezioni (PE Headers)

L'analisi delle sezioni rivela anomalie strutturali che indicano che l'eseguibile è stato manipolato o "impacchettato" (Packed).

3.1 Anomalie Rilevate

Dalla tabella delle sezioni emergono i seguenti indicatori di compromissione:

1. **Duplicazione delle Sezioni:** Sono presenti sezioni con nomi duplicati (es. due sezioni `.text` e due `.rsrc`), indicando una possibile iniezione di codice post-compilazione.
2. **Permessi RWX (Sezione .text critica):** La sezione identificata come `section[3]` (.text) presenta permessi simultanei di **Scrittura (Write)** ed **Esecuzione (Execute)**.
   - Questa configurazione viola le policy di sicurezza standard (W^X).
   - Permette al codice di modificarsi durante l'esecuzione (Polimorfismo).
3. **Alta Entropia:** La stessa sezione presenta un valore di entropia pari a **6.428**. Sebbene non altissimo, combinato con il flag *Self-modifying*, suggerisce la presenza di codice offuscato o compresso per evadere l'analisi antivirus.

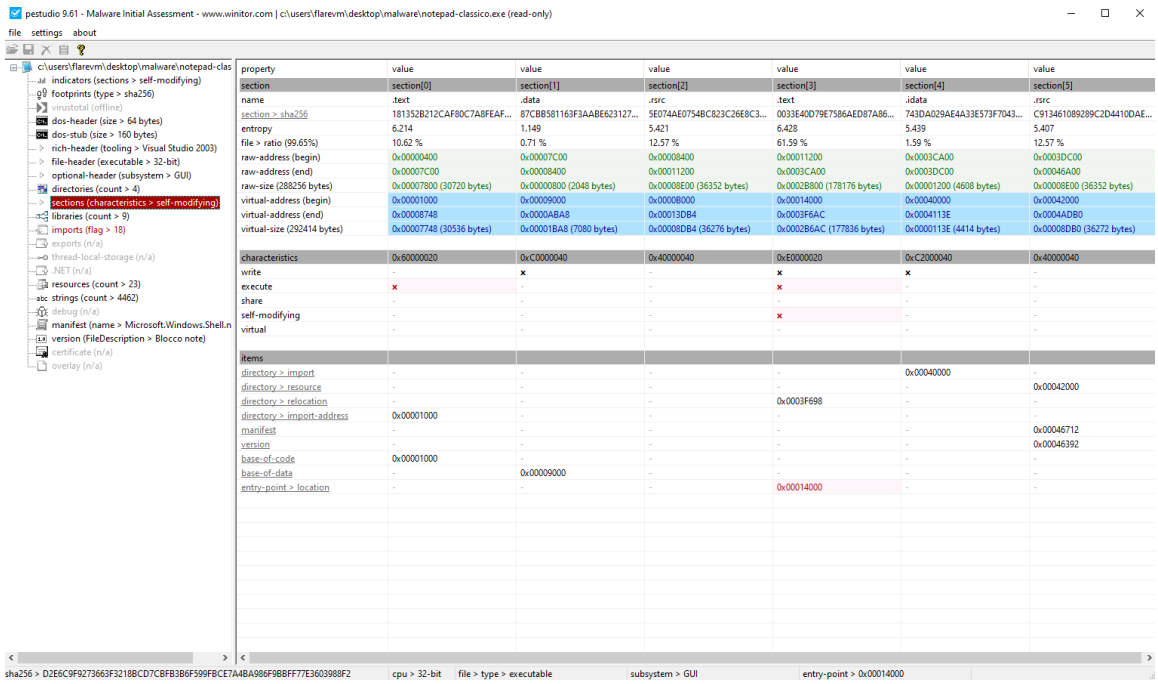


Figura 2: Analisi delle sezioni: evidenziati permessi RWX e flag self-modifying.

4 Conclusioni

L'analisi statica conferma che `notepad-classico.exe` non è un semplice editor di testo. Le evidenze raccolte mostrano:

- **Capacità malevole:** Accesso al registro per persistenza, manipolazione file e memoria.
- **Tecniche di evasione:** Struttura del file anomala (sezioni duplicate) e permessi RWX che suggeriscono l'uso di packer o codice polimorfico.

Si raccomanda di non eseguire il file in un ambiente di produzione e di procedere con l'analisi dinamica in Sandbox.